LATERAL NEWS — LATERALCODE

Tecnologia ed evoluzione: sei uno Zero Trust o uno ZeroSurface®?

16 maggio 2023

Lo abbiamo letto e sentito non sappiamo più quante volte: “la pandemia di COVID19 ha rivelato e amplificato le debolezze delle politiche di sicurezza informatica in aziende, istituzioni e fornitori di servizi IT”. La buona notizia è che siamo stati costretti a osservare con occhio critico, meglio sarebbe stato se impietoso, le politiche di **sicurezza informatica** del Bel Paese e non solo.

PARLANDO DI NOVITÀ

Nel vivace panorama che si è delineato sembra aver riscosso grande attenzione e molti sostenitori (non sapremmo misurarne il successo) la linea *Zero Trust*.

Zero Trust è un *concept*, una **configurazione ideale**, una (ri)strutturazione organica di diversi *layer* connessi tra loro, una composizione dinamica di strumenti, tecniche e progettazione. Molti grandi player hanno sposato il disegno, o **dichiarano di volerlo fare**: Cisco, Check Point, Akamai, Google, Symantec, Unisys, Illumio e altri ancora, ciascuno con una particolare attenzione o predilezione per certi aspetti invece che per altri, preferenze in parte guidate, immaginiamo, dalle proprie competenze, strategie e vocazioni.

Quel che è certo è che su alcuni principi sembrano convenire un po' tutti come, per es., l'eliminazione delle VPN (noi lo diciamo da tempo), l'integrazione delle funzionalità di SIEM (Security Information and Event Management), la gestione degli accessi in MFA (Multifactor Authentication) e in SSO (Single Sign-On, questo ci piace meno), l'abilitazione delle soluzioni WFA (Web Application Firewall) e altro ancora.

Facendo un passo indietro però non è difficile rilevare (come per altro dichiarato da tutti gli attori coinvolti, e ci mancherebbe) quanto questa rinnovata attenzione sia dovuta all'esponenziale aumento delle superfici esposte dei sistemi, condizione che, con piena evidenza, è da sempre alla base di uno dei più grandi nodi della sicurezza informatica: se non ci fossero superfici esposte, infatti, esisterebbero molti meno problemi. Per contro però se non fosse garantita la raggiungibilità (e quindi, ahinòi, l'esposizione), non sarebbero garantiti neanche i servizi offerti in rete (perlomeno questo è quanto abbiamo sempre creduto).

Sotto questo profilo, dunque, niente di nuovo "dal cielo dello *Zero Trust*".

CURIAMO IL SINTOMO O LA CAUSA?

Partecipando a convegni, leggendo *paper* e articoli di varia estrazione, ascoltando tecnici ed esperti e così via, ci sembra di capire che l'esposizione delle superfici (e la loro moltiplicazione) sia considerata come un inevitabile prezzo da pagare, qualcosa con cui dobbiamo convivere *obtorto collo*, non più oggetto di approfondimento e vera ricerca; per il mondo dei servizi e delle applicazioni pubblicate, passando per l'IoT e l'universo delle API, insomma, la faccenda è chiusa, resta così com'è.

Nel racconto più diffuso, la **protezione perimetrale** pare un argomento sorpassato, quasi "vintage" per usare un termine tanto in voga, ineluttabilmente irrisolvibile, un male necessario; e siccome i racconti sono fatti di (tante) parole, ecco, per es., l'orribile "deperimetralizzazione" - che poi racconta una storia diversa da quella per cui viene usata (un *concept*, per di più, vecchio di vent'anni, v. Jericho Forum).

In ogni caso, l'argomento "esposizione" appare privo di quella **pseudo-modernità di pensiero** che, in maniera del tutto autoreferenziale, sembra dover caratterizzare le soluzioni affinché queste assumano la commercialmente necessaria aura di credibilità, efficacia e validità; al che verrebbe da pensare come trovi diritto di cittadinanza, in quel novero, proprio lo *Zero Trust*, considerando che la sua prima formulazione risale al 2010, non proprio di primo pelo insomma (in fondo però stanno tornando di moda anche i pantaloni a zampa d'elefante ■, magie dei cicli e del marketing).

Parliamoci chiaro; c'è merito e valore nelle soluzioni che via via ci vengono proposte, ma crediamo anche che aver archiviato così frettolosamente la questione "superfici esposte" sia, in realtà, una dichiarazione di resa, un'ammissione di impotenza quando invece, se risolta, cambierebbe lo scenario in maniera drastica, ridisegnandolo completamente.

Se a questo aggiungiamo che le superfici esposte non sono solo quelle all'**esterno** di una rete ma anche quelle al suo **interno** (questione di architettura!) — e anche quelle di TUTTI i sistemi

di sicurezza oggi disponibili — beh, liquidare così l'argomento rischia di farci perdere un'occasione importante di eliminare parecchi problemi alla radice.

D'altro canto è proprio questo problema irrisolto che giustifica buona parte degli investimenti e muove il mercato dell'offerta.

Ci piace lo *Zero Trust*, soprattutto nel suo approccio organico e "multidisciplinare", ma ci convince meno proprio l'innalzamento di quella bandiera bianca: fintanto che non sarà risolto "IL" problema, infatti, ci sentiamo di dire che la locuzione *Zero Trust* peccherà suo malgrado di "incoerenza" dovendosi nel frattempo riformularsi, a nostro giudizio, in un più aderente *Less Trust Possible*.

MODA vs. CONTENUTI

Il principio di "nessuna fiducia" è invece intrinseco allo **ZeroSurface®**, ne è il **nucleo funzionale**, tanto imprescindibile quanto pienamente raggiunto.

Un sistema **ZeroSurface®** ha sempre l'intero mondo in blacklist, in qualunque stato operativo esso si trovi!

Per quanto blinderai una porta ci sarà sempre un ariete in grado di abbatterla, per quanto innalzerai muri ci sarà sempre un modo per scalarli.

Leggiamo obiezioni secondo cui una simile difesa perimetrale comporterebbe:

- una gravosa gestione di complicati *appliance*;
- aggiornamenti continui dei software (che in effetti, se l'obiezione fosse valida, aumenterebbero la complessità totale e quindi la comparsa di comportamenti emergenti, altro micidiale problema che affronteremo in una prossima edizione della newsletter);
- un aumento del carico di lavoro per i team IT;
- relativo aumento dei costi

Ora qualche domanda: le altre soluzioni, di diverso orientamento, non comportano forse i **medesimi** oneri?

E poi: davvero possiamo ignorare il problema o conviverci da separati in casa solo perché finora non abbiamo saputo come affrontarlo?

E se, invece, esistesse un modo per evitare tutto quel carico di costi economici, strumentali e di lavoro?

E, *last but not least*, che senso avrebbe ignorare il problema proprio adesso che è stato risolto?

Sì, avete letto bene: **RISOLTO**.

LA SEMPLICITÀ È LA SOFISTICAZIONE SUPREMA

Se *Zero Trust* è una dichiarazione di intenti, *ZeroSurface*® è una realtà concreta e **realmente innovativa**.

Se *Zero Trust* è un concept, *ZeroSurface*® — azzeramento delle superfici esposte — è una tecnologia **brevettata**.

Se *Zero Trust* è un percorso destinato a una laboriosa implementazione di medio periodo, una condizione di *ZeroSurface*® si raggiunge **in pochissimo tempo** (da poche ore a qualche settimana nei casi più complessi).

Se *Zero Trust* è rincorsa continua, aggiornamenti, affinamenti e controlli quotidiani, stratificazione di tecnologie, strumenti e dispositivi, *ZeroSurface*® è **efficienza e semplicità sistemiche**.

E quando parliamo di semplicità non parliamo di semplificazione forzata, a tutti i costi (otto anni di sviluppo della tecnologia sono lì a dimostrarlo), ma di un approccio sistemico e non sintomatico al problema.

> *Complicare è facile, semplificare è difficile. Per complicare basta aggiungere, tutto quello che si vuole: colori, forme, azioni, decorazioni, personaggi, ambienti pieni di cose. Tutti sono capaci di complicare. — Bruno Munari*

Zero Trust è un interessante tentativo di prendere quel che c'è al momento nel grande contenitore delle proposte di sicurezza informatica, eliminare ciò che è "inadeguato" e creare una piattaforma concettuale composita, popolata da molteplici soluzioni e operatori: senz'altro un importante **progresso**, un riordino degno di Marie Kondo.

Ma questo è il punto.

ZeroSurface® è **evoluzione**, non solo progresso!

iceGate, la soluzione *ZeroSurface*® di LATERALCODE, non rientra in nessuna "famiglia" già esistente: non è un firewall, non è una VPN, non è SIEM, non è un WFA, non è un Identity Provider né altro, iceGate è la comparsa di una nuova specie, una soluzione di sicurezza informatica asincrona, asimmetrica, multifattore e… a superficie zero, appunto.

QUINDI ZERO TRUST O ZeroSurface®?

Dobbiamo confessarlo, la domanda del titolo è provocatoria poiché *Zero Trust* e *ZeroSurface*® non sono mutualmente esclusivi, possono anzi essere ottimi componenti della stessa squadra.

Tuttavia, in conclusione, permetteteci una domanda: se da un lato lo *ZeroSurface*® può esistere senza lo *Zero Trust* ma mantenere ugualmente la promessa racchiusa nel proprio nome, il contrario è forse possibile?

Lateral News — Articoli, idee e riflessioni sullo sviluppo tecnologico e sulla sicurezza informatica non “mainstream”

lateralcode.it